(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 494 796 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
15.04.1998 Bulletin 1998/16

(51) Int Cl.[6]: **G07F 19/00**, G07C 9/00

(21) Application number: **92300241.4**

(22) Date of filing: **10.01.1992**

(54) Transaction recording apparatus and method

Vorrichtung und Verfahren zur Aufzeichnung von Transaktionen

Dispositif et méthode pour l'enregistrement de transactions

(84) Designated Contracting States:
DE FR GB

(30) Priority: **11.01.1991 US 640199**

(43) Date of publication of application:
15.07.1992 Bulletin 1992/29

(73) Proprietor: **NCR International, Inc.**
Dayton, Ohio 45479 (US)

(72) Inventors:
- **Kapp, Michael Alan**
  New Philadelphia, Ohio 44663 (US)
- **Protheroe, Robert Llewellyn**
  Cambridge, Ohio 43725 (US)
- **Onega, Albert Michael**
  Lore City, Ohio 43755 (US)

(74) Representative: **Irish, Vivien Elizabeth**
International IP Department,
NCR Limited,
206 Marylebone Road
London NW1 6LY (GB)

(56) References cited:
WO-A-85/00683
WO-A-91/10207
FR-A- 2 592 197
GB-A- 2 053 617

EP 0 494 796 B1

Printed by Jouve, 75001 PARIS (FR)

Description

This invention relates to an apparatus and method of recording a transaction, and in particular, but not exclusively, to an apparatus and method for processing signature-based payment transactions, and more particularly, to an apparatus and method in which a merchant's records of payment may be generated and maintained electronically without generation or use of paper records except those delivered to customers at the point of sale.

In retailing and similar areas, the volume of transactions is often such that management of paper records is burdensome. Therefore paper records are being replaced by digital storage media wherever feasible. However, digital storage devices have not been able to eliminate the need for paper storage in many financial transactions requiring consumer approval. Typical examples are transactions involving account debit (including check) and charge receipts. In such transactions paper documentation bearing a human signature has continued to be the norm. The storage and retrieval of such records is both inefficient and costly.

Known techniques exist for producing digitized facsimiles of human signatures and processing such digitized facsimiles to verify the authenticity thereof, as disclosed in US patents 4752 965, 4734 859, 4724542. An apparatus for electronically processing a transaction with a human signature is known from WO-A-9110207 (publication date : 11.07.91) where a digitized signature signal is combined with a digitized transaction signal to form a record signal which is then processed for verification of the transaction.

The present invention seeks to enhance the security and reliability of the approval and recordal of transactions carried out by electronic means. According to the present invention, there is provided transaction recordal apparatus comprising first generating means for generating a digitized signature record of a signature approving said transaction, characterized by second generating means for generating a digitized transaction record representative of said transaction, and means for using said transaction record to encrypt said signature record so as to provide an encrypted record for supply to signature and transaction verification means.

The invention also provides a method of recording a transaction, comprising the steps of generating a digitized signature record of a signature approving the transaction, and generating a digitized transaction record representative of the transaction characterized by the step of generating an encrypted record of the transaction for supply to signature and transaction verification means by using said transaction record to encrypt said signature record.

The invention advantageously provides for a practical method and apparatus for capturing an image of a signature in digital form and combining it with a digital record of the transaction itself so as to provide an encrypted record of the transaction. Thus, the apparatus and method provide for an effective defence against attempted fraud. In particular, the invention can assure that a signature purportedly approving a commercial obligation was captured at the time of a questioned transaction and is not a genuine signature obtained on some other occasion and fraudulently merged into the digital record of the transaction.

Also, the present invention provides for a method and apparatus for processing signature-based payment transactions by use of digitized representations of payment documents.

Further advantages arise in that a method and apparatus are readily provided for generation and signature of an electronic payment document which is easily usable by and readily acceptable to a customer. Also, electronic generation and electronic signature of a payment document with sufficient security to obviate the need for maintenance of paper records are provided which also allows for the generation of a digital record of a commercial transaction which is secure from tampering.

The invention is described further hereinafter, by way of example only, with reference to the accompanying drawings in which:-

Fig. 1 is a perspective view of a write input apparatus and associated printer.

Fig. 2 is a sectional elevational view of the write input apparatus of Fig. 1.

Fig. 3 is a plan view of a liquid crystal display module which is used in the write input apparatus of Fig. 1.

Fig. 4 is an elevational view of the liquid crystal display module of Fig. 3.

Fig. 5 is a block diagram of a point of sale system which includes the write input apparatus of Fig. 1.

Fig. 6 is an illustration of a combined bill of sale and credit receipt printed at a point of sale.

Fig. 6A is an illustration of a debit memo produced at a point of sale.

Fig. 7 is a flow chart illustrating the production of a digitized transaction record such as the debit memo of Fig. 6A.

Fig. 8 is a flow diagram of the process employed to transform the coordinates of a position of a transparent digitizer to the corresponding coordinates of a display module.

Fig. 9 is flow diagram of the process employed to provide offset values used in the process of Fig. 8.

Reference is now made to Fig. 1, wherein there is shown a perspective view of a write input apparatus 20 which is coupled to a printer 22 by a connector 21. Although this is shown as a direct connection or coupling, the actual coupling or connection may actually extend through one or more other devices, such as a controller. The write input device includes a transparent surface 24 through which information may be displayed and on which information may be entered by writing thereon with a stylus 26 by a human operator 28. The stylus 26 is connected to the apparatus

by an electrically conductive line 30. The apparatus 20 may also include an integral magnetic stripe reader 32 having a slot 34 through which a card bearing magnetic indicia may be swiped so that the data contained thereon may be read, stored and used by the system. The write input device 20 may be configured without the magnetic stripe reader 32, if desired. Thus the present invention contemplates the use of a device for manual data entry instead of or in addition to the magnetic stripe reader. Also, the system may include a MICR reader for reading magnetically imprinted characters on a customer's personal check. This would enable the use of a personal check for identification of a customer's checking account number.

Printer 22 may print customer receipts such as the receipt 36 which is shown as issuing from an aperture 38 in the housing of the printer. Details of receipt 36 may be as illustrated in Fig. 6. Other types of records could also be generated by the printer 22, if desired, in response to the needs of the system. Any suitable printer may be employed, such as an Epson RP265, marketed by Epson America, Inc., Torrance, California.

As shown in the sectional view of Fig. 2, write input apparatus 20 has a lower housing 40 and an upper housing 42, which mate along the edges thereof. The upper housing 42 has an aperture 44 within which is placed a transparent interactive digitizer element 46 which is capable of generating electrical signals which represent the position of the stylus 26 or other device placed in contact therewith. Broadly speaking, during operation of the interactive element 46, the stylus 26 acts as a probe and the differing potentials between sides of the element, in two coordinate directions, are measured, converted into digital form, and are processed through correction algorithms. This enables a trace of the movement of the stylus to be captured and retained, as well as displayed on a liquid crystal display (LCD) module 48. Interactive elements of this type are commercially available, and one such device which can be employed in the present invention is the ScreenWriter controller/digitizer/pen marketed by MicroTouch Systems Inc., Wilmington, Massachusetts.

Positioned directly beneath the interactive transparent element 46 and having a display screen visible therethrough is the liquid crystal display (LCD) module 48 which is capable of displaying information in response to electrical signals applied thereto. Information which is read from a card by the magnetic stripe reader 32, or input by a Magnetic Ink Character Recognition (MICR) device, or manually entered through a keyboard may be supplied to and displayed by the LCD module 48. Also, a magnetically encoded card or a keyboard may be used for accessing a look-up table in a memory to generate information for displaying graphics on the screen of the LCD module 48. Electrical signals from the interactive element 46 relating to movement of the stylus 26 on the element can then be applied to the LCD module 48 to provide a representation of a signature on the transaction image. Thus, since the LCD module 48 is positioned directly beneath the transparent digitizer element 46, the movements of the stylus 26 on the transparent surface 24 are graphically captured and are immediately visible at the points of contact of the stylus with the surface. Other transaction information may also be manually entered via the write capture surface in the same manner as the signature except that its position is correlated to an input grid displayed through the transparent surface for input prompt, e.g., numeric keypad image. Such information is recognized from its position and is digitized accordingly.

Figs. 3 and 4 are plan and elevation views of the LCD module 48. A display screen 50 forms part of the top surface of the module. A cable 52 provides electrical input connections for supplying power and data signals to the module. Electrical conductors 53 provide power to fluorescent tubes for back-lighting the screen 50. Brackets 54 are secured to the module to enable it to be mounted securely within the apparatus 20. LCD modules of this type are commercially available, and one such module which can be employed in the present invention is Model EG7500, marketed by Epson America, Inc., Torrance, California.

The magnetic stripe reader 32 and its slot 34 are shown to be located in the upper left portion of the apparatus 20, as viewed in Fig. 2. A control circuit board 56 which functions as a controller for the transparent digitizer element 46 is located below the LCD module 48 in the lower housing 40 of the apparatus 20 and includes a connector 57 for connection to the digitizer element 46 and also includes a microcontroller 64. Circuit board 56 may include circuitry for automatically adjusting the contrast control signal applied to LCD module 48 to correct for temperature induced variations in the contrast of the display.

A point of sale system using the present invention is illustrated in block diagram form in Fig. 5. The system as shown therein includes the write capture unit 20, a transaction terminal 13 and the optional standalone printer 22. MSR 32 which is shown in phantom outline within write input unit 20 may be integrated as part of that unit or may be a standalone device. An optional MICR reader 58 is also shown in phantom outline. The transaction terminal 13 may be any one of a number of commercially available devices, such as, for instance, a 7052 terminal, marketed by NCR Corporation. The optional standalone printer may be of any suitable dot matrix printer offering an RS232 interface, such as the NCR 7150 printer.

Terminal 13 controls the functioning of write input device by means of commands sent over a serial data link 14. These control commands are received by an input/output buffer 29 and relayed to a microprocessor based I/O controller 33 for routing to the microcontroller 64. Microcontroller 64 runs one or another of four different programs, as selected by control messages from terminal 13. Basically, there are four types of messages:

DISPLAY
ACCEPT
TRANSMIT
UPDATE

DISPLAY messages may include character codes for characters to be displayed by LCD module 48. These codes are sent by microcontroller 64 to LCD controller 47, which may be, for instance a Display Master Model YDM420 graphics adapter marketed by Yamaha Corporation of America, San Jose, California. LCD controller 47 then converts the character codes into row and column commands for displaying the desired characters in dot matrix form. Alternatively, DISPLAY messages may cause microcontroller 64 to access its own memory for character codes stored therein and send those codes to LCD controller 47 for display.

ACCEPT messages activate logic that causes microcontroller 64 to sense the activation of stylus 26 and begin accepting X,Y coordinate from digitizer 46. This information is captured and "echoed" to the LCD 48 to provide a signature display to the signer in "real time".

Receipt of a TRANSMIT message initiates transmission of the signature information to the transaction terminal along with other account information obtained from the debit card read by the MSR 32. (MSR input is also controlled via ACCEPT messages.) Encryption means 49 are provided for encrypting the signature information prior to transmission to terminal 13. Encryption means 49 may be implemented either in hardware or in software.

The UPDATE messages are used for causing microcontroller 64 to update its memory with display information for use in controlling printer 22.

Upon receipt of the signature information, the terminal may send the data over communication links to a validation point for signature validation and transaction approval. Validation may be done by the human eye or by automatic signature recognition equipment. The electronic charge or debit draft information is stored locally on disk 15 for later retrieval and batch transmission to an Automated Clearing House (ACH) or other financial institution for processing. Storage is in encrypted form. For customer records, paper media of the transaction may be provided either by the terminal 13 or optionally by printer 22. A printer interface unit 23 may be provided for this purpose.

As hereinafter described in detail, a uniform message format is used in messages from terminal 13 to I/O controller 33. This message includes a one-byte field BCC which is created by performing an EXCLUSIVE OR operation on other fields which specifically identify the transaction. BCC may be used as an encryption key for encoding the digitized signature and other transaction data, as desired.

In the preferred embodiment of the invention only the signature is encrypted so as to enable the system to be used in an environment including a wide variety of other types of electronic debit equipment. It is contemplated that a transaction-specific encryption key, such as BCC, will be used so as to associate the signature with a particular transaction and thereby discourage fraudulent use of a signature which may have been obtained legitimately in connection with a different transaction. By way of example an account debit may be made in reliance upon an electronically captured signature as illustrated in Fig. 6A.

Fig. 6A represents an LCD display which may be created in connection with a debit transaction or a hard copy thereof as printed by printer 22. It will be seen that the display includes a transaction code consisting, for example, of two hexadecimal words FB3C and 27A6. The first word might identify a particular merchandising location and perhaps a time identifier, whereas the second word could be a sequentially assigned number. Thus the code could refer to transaction number 27A6 by store number FB during week 3C.

The authorizing signature is captured dynamically as a series of time related X-Y coordinates during actual writing by the customer. This provides a much better record for later verification than a frozen, picture-type signature of the type produced by ordinary bit-mapping. Capturing of the signature begins upon contact of the stylus 26 with digitizer screen 46, at which time a pair of starting coordinates, Start X and Start Y are generated. These coordinates are compared with a series of subsequent coordinates Touch X and Touch Y which are sensed at regularly timed intervals. The X and Y differences are stored as a series of digital words.

After the signature is captured it is encrypted in two phases. In the first phase the two words of the transaction code are subjected to an exclusive OR operation (XOR) to obtain a single word encryption key; in this case the key is found to be DC9A. This key then is XORed against the signature data to obtain an encrypted signature file. This effectively imbeds the transaction identification code into the signature.

The second phase of the encryption process adds security by using a sophisticated encryption technique such as the Data Encryption Standard (DES) issued by the U.S. National Bureau of Standards. This phase uses secure encryption keys known only to the merchant and the financial institution.

At the time of posting the financial institution will first decrypt the DES encryption. Then, since the basic transaction data has not been encrypted, the transaction code may be read and XORed to obtain the DC9A XOR key. This key then is XORed against the signature file to obtain a readable copy of the authorizing signature. Since the signature copy cannot be produced except with the aid of the transaction code, the financial institution knows that the signature

was written at the time of the transaction. Consequently the financial institution may safely debit the customer's account for the amount of the transaction. Of course, it is also necessary for the financial institution to authenticate the decrypted signature by comparing it against a sample signature obtained upon opening the account. As noted above, the dynamically recorded signature file obtained through use of this invention facilitates automatic signature recognition.

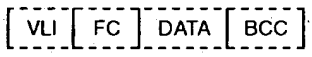
A "C" language routine for accomplishing the above described EXCLUSIVE OR operation is taught in "Advanced Turbo C", 2nd Ed, Herbert Schildt, Borland Osborne/McGraw- Hill 1989 at pp. 265, 266. DES encryption is well known. It uses a 64 bit key and is best performed by a specially configured "hardware" encoder. However, it may be carried out in software, if desired. An example of a software implementation of DES encryption in "C" language is given in "Numerical Recipes in C, The Art of Scientific Computing", Press et al. Cambridge University Press, 1989, pp. 228-236.

The manner in which the system performs a point of sale transaction will now be described with reference to the flow diagram of Fig. 7. As illustrated therein, the sequence begins at start block 150 which is the powerup condition. The idle screen, as defined by the processor program is displayed (152). The idle loop continues until a message is received from the terminal, block 54. The message can be any of the four general types mentioned above. The type of message is identified by the decision three indicated at 156, 158, 160 for DISPLAY, ACCEPT and TRANSMIT. A failure at all three points produces an UPDATE response, as shown at 162. If the message is a DISPLAY message, the information in the message, or the stored information designated by the message, is displayed on the LCD 64. The program then returns to the idle loop.

If the message is of the ACCEPT type, then the program checks to determine whether the input is to be via MSR or stylus input (165). If it is to be by stylus, then the program checks for stylus activation (166). If the stylus has been activated, the system proceeds to capture the signature data and echo to the LCD (block 168). This continues until a terminal command or a stylus deactivation indicates that the data entry is complete (170). If the test at 165 indicates that data is to be accepted from the MSR then the system proceeds to block 167 where the magnetic data is read. When the magnetic input is complete, the information is stored and the program returns to idle loop.

If the message is of the TRANSMIT type, the program checks (172) to determine whether the message is a print command. If so, a check is made at 174 to determine whether the printing is to be done by the standalone printer or by the terminal. At this point the transaction data is formatted and printed by the appropriate device as shown at block 178 and 179. Thereafter if the test at 172 indicates that the message is not a print instruction, the program determines if encryption is required (176). The transaction data is encrypted, if appropriate (180) and sent to the terminal (182). Thereafter the program returns to the idle loop. If the message is of the UPDATE type, the specific request is determined and appropriate action is taken after which the program returns to the idle loop.

A common format is used for all messages from terminal 13. It is as follows:



where:

VLI is a two-byte length of the data portion of the message. The first byte of the VLI field is the upper eight bits of the data field length and the second byte is the lower eight bits of the data field length.

FC is a one-byte function code which specifies the message type and the particular function to be performed. DATA is a variable length field of characters that are associated with the function code. This is an optional field and may not be present in every message.

BCC has been mentioned above and is a one-byte field that is the EXCLUSIVE OR of the VLI, FC, and DATA fields.

Responses by write capture unit 20 to terminal 13 follow the same format with exception that the FC field is used to return the status of the operation that was requested. The DATA field is also an optional field that may or may not be transmitted to the terminal depending on the type of response.

The following are examples of various message types:

Message Type	Codes	Function Description
Transmit	01	Transmit Encrypted Signature Record
Transmit	02	Transmit Printable Signature Data
Accept	03	Accept Signature Data
Transmit	04	Transmit x, y Touch Screen Data
Transmit	05	Resend Last Response

(continued)

Message Type	Codes	Function Description
Update	06	Signature Completion Indication
Transmit	07	Transmit Diagnostic Tallies
Transmit	08	Transmit Firmware/Software Identification
Update	09	Reset Write Capture Unit (Perform Level 0 Diagnostics)
Update	OA	Accept New Program Load
Accept	OB	Accept MSR Data
Accept	OC	Accept MICR Data
Display	11	Display Stored Image #1
Display	12	Display Stored Image #2
Display	13	Display Stored Image #3
Display	22	Display Full Screen #1
Display	23	Display Full Screen #2
Display	31	Enter Customer Display Mode
Display	32	Display Text (Custon;er Receipt) Data
Accept	41	Accept Card Image #1 Data
Accept	42	Accept Card Image #2 Data
Accept	43	Accept Card Image #3 Data
Accept	52	Accept Full Screen #1 Data
Accept	53	Accept Full Screen #2 Data
Update	71	Receive Encrypted Working Key
Update	72	Receive Key Exchange Key
Update	77	Receive/Continue Load for Key Exchange Key
Transmit	78	Transmit for Key Status
Update	81	Perform Communications Turnaround Test
Update	Al	Perform Battery Test
Update	D1	Download Record to LCD Memory
Update	D6	Download Record to Processor Memory
Update	DC	Download Character Set
Update	D8	Echo Data to LCD from MSR, Digitizer or MICR Card

In order to display stylus generated information on the LCD module 48, it is necessary to transform the digitizer coordinates into the coordinate system of the LCD module. This process is performed by the PC controller 64. The process used to accomplish this transformation is illustrated in the flow diagram of Fig. 8. Performance of this process is dependent upon obtaining certain constants which are used in equations for this transformation. The process for obtaining these constants is shown in Fig. 9, which will be described subsequently.

The process of Fig. 8 begins with start block 210, and then proceeds to block 212 in which an inquiry is made as to whether the stylus 26 is touching the digitizer 46. The process does not continue until the stylus does touch the digitizer. When the stylus 26 is touching the digitizer 46, the process continues to block 214, in which the transparent digitizer coordinates "touch X" and "touch Y" are determined and transmitted by the transparent digitizer controller included in block 56 to the PC controller 64. These coordinates represent the instantaneous position of the stylus 26 on the screen 50, taken at periodic time intervals during movement of the stylus 26.

The corresponding positional coordinates "lcd X" and "lcd Y" for the LCD module 48 are then calculated from "touch X" and "touch Y", as represented in block 216. This transformation is accomplished by use of the following equations:

1. lcd X= mx * touch X + bx

2. lcd Y= my * touch Y + by

where

lcd X, lcd Y are display coordinates,
touch X, touch Y are digitizer coordinates,
mx, my are scalar constants,
bx, by are offset constants.

The method for determining mx, my, bx and by will be described subsequently in connection with the flow diagram of Fig. 9.

The process continues to block 218 where lcd X and lcd Y are described on LCD module 48. An inquiry is then made (block 220) as to whether a "signature complete" indication has been made, which may be indicated a signal generated in the write input apparatus 20 when the signer places the stylus in a designated holder. If the signature is complete, the process is concluded (block 224). If the signature is not complete, the process continues via path 222 to block 212.

The constants mx, my, bx and by are determined in accordance with the process set forth in the flow diagram of Fig. 9, which proceeds from the start position 230 to display a first point at predetermined LCD module screen coordinates "lcd X1" and "lcd Y1", as represented in block 232. The user then touches this displayed point with the stylus 26, thus yielding corresponding digitizer coordinates "touch X1" and "touch Y1", as represented in block 234. A second predetermined point, physically spaced from the first predetermined point, at coordinates "lcd X2" and "lcd Y2" is then displayed (block 236). The user then touches this second displayed point with the stylus 26, thus yielding corresponding digitizer coordinates "touch X2" and "touch Y2", as represented in block 238. For maximum accuracy, the tiro predetermined points should be at opposite corners of the planned active area of the screen of the LCD module 48.

The quantities mx, my, bx and by are then determined, as represented in block 240, in accordance with the following equations:

$$3.\quad mx = (lcd\ X1 - lcd\ X2) / (touch\ X1 - touch\ X2)$$

$$4.\quad b\ x = lcd\ X1 - mx * touch\ X1$$

$$5.\quad m\ y = (lcd\ Y1 - lcd\ Y2) / (touch\ Y1 - touch\ Y2)$$

$$6.\quad b\ y = lcd\ Y1 - my * touch\ Y1$$

These constants (mx, my, bx and by) are then stored and used to calculate display coordinates from any subsequent digitizer coordinates, as per block 242. The process is then concluded at block 244.

The system and method of the present invention have been disclosed herein primarily in connection with an arrangement for signature-based payment transactions. However the invention is not limited to such an arrangement and could be used in connection with other transactions requiring authorization by a digitized signature. This might include, for example, a written order for a public servant to perform an official act.

It will also be appreciated that while a method and apparatus have been disclosed for creating a transaction-specific encryption of a signature, the invention contemplates quasi specific encryption such as could be accomplished by use of an encryption key which is changed frequently so as to enable an encrypted signature to be correlated with time.

Claims

1. Transaction recordal apparatus comprising first generating means (20) for generating a digitized signature record of a signature approving said transaction, characterized by second generating means for generating a digitized transaction record representative of said transaction, and means (49) for using said transaction record to encrypt said signature record so as to provide an encrypted record for supply to signature and transaction verification means.

2. Apparatus according to claim 1, characterized by means for performing a second encrpytion of said digital record

using a predetermined encryption key.

3. Apparatus according to claim 1 or 2, characterized in that said first generating means comprises a manually operated stylus (26), and a digitizer (46) for sensing and digitizing the coordinates of said stylus (26).

4. Apparatus according to claim 3, characterized by display means (48) for presenting a visual image corresponding to said signature.

5. Apparatus according to claim 4, characterized in that first generating means (20) comprises a transparent reference surface (46) for generating position sensing signals in response to moving contact by said stylus (26) which is mounted on a liquid crystal display (48) for causing said visual image to be presented in registration with successive points of contact between said surface (46) and said stylus (26).

6. Apparatus according to claim 5, characterized by display means (50) for displaying a visual image corresponding to said transaction.

7. A method of recording a transaction, comprising the steps of

generating a digitized signature record of a signature approving the transaction, and
generating a digitized transaction record representative of the transaction

characterized by the step of
generating an encrypted record of the transaction for supply to signature and transaction verification means by using said digitized transaction record to encrypt said signature record.

8. A method according to claim 7, characterized in that the step of generating an encrypted record of the transaction includes selecting data from said digitized transaction record and exclusive ORing said data against said digitized signature record.

Patentansprüche

1. Vorrichtung zur Aufzeichnung von Transaktionen, aufweisend
eine erste Erzeugungseinrichtung (20) zum Erzeugen einer digitalisierten Unterschriftenaufzeichnung einer Unterschrift, mit der die Transaktion genehmigt wird,
gekennzeichnet durch
eine zweite Erzeugungseinrichtung zum Erzeugen einer diese Transaktion darstellenden digitalisierten Transaktionsaufzeichnung und eine Einrichtung (49), die die Transaktionsaufzeichnung zur Chiffrierung der Unterschriftenaufzeichnung verwendet, um eine chiffrierte Aufzeichnung zur Lieferung an eine Unterschriften- und Transaktionsnachweiseinrichtung bereitzustellen.

2. Vorrichtung nach Anspruch 1, gekennzeichnet durch eine Einrichtung zum Durchführen einer zweiten Chiffrierung der digitalen Aufzeichnung unter Verwendung eines vorbestimmten Chiffrierungsschlüssels.

3. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die erste Erzeugungseinrichtung einen von Hand geführten Schreibstift (26) und einen Digitalumsetzer (46) zum Abtasten und Digitalisieren der Koordinaten des Schreibstiftes (26) aufweist.

4. Vorrichtung nach Anspruch 3, gekennzeichnet durch eine Anzeigevorrichtung (48) zum Darstellen eines der Unterschrift entsprechenden visuellen Bildes.

5. Vorrichtung nach Anspruch 4, dadurch gekennzeichnet, daß die erste Erzeugungseinrichtung (20) eine transparente Bezugsfläche (46) zum Erzeugen von Positionsabtastsignalen unter Ansprechen auf einen Bewegungskontakt durch den Schreibstift (26) aufweist, die auf einer Flüssigkristallanzeige (48) befestigt ist, um zu bewirken, daß das visuelle Bild durch Registrierung aufeinanderfolgender Kontaktpunkte zwischen der Fläche (46) und dem Schreibstift (26) dargestellt wird.

6. Vorrichtung nach Anspruch 5, gekennzeichnet durch eine Anzeigeeinrichtung (50) zur Anzeige eines der Trans-

aktion entsprechenden visuellen Bildes.

7. Verfahren zur Aufzeichnung von Transaktionen, mit den Schritten:

- Erzeugen einer digitalisierten Unterschriftenaufzeichnung einer Unterschrift, mit der die Transaktion genehmigt wird; und
- Erzeugen einer die Transaktion darstellenden digitalisierten Transaktionsaufzeichnung

gekennzeichnet durch den Schritt:

- Erzeugen einer chiffrierten Aufzeichnung der Transaktion zur Lieferung an eine Unterschriften- und Transaktionsnachweiseinrichtung, wobei die digitalisierte Transaktionsaufzeichnung zur Chiffrierung der Unterschriftenaufzeichnung verwendet wird.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß der Schritt Erzeugen einer chiffrierten Aufzeichnung der Transaktion das Auswählen von Daten aus der digitalisierten Transaktionsaufzeichnung und das Setzen dieser Daten in Antivalenz zu der digitalisierten Unterschriftenaufzeichnung einschließt.

Revendications

1. Un appareil d'enregistrement des transactions comprenant un premier moyen de génération (20) pour générer un enregistrement de signature numérisé d'une signature approuvant ladite transaction, caractérisé par un deuxième moyen de génération pour générer un enregistrement de transaction numérisé représentatif de ladite transaction, et un moyen (49) pour utiliser ledit enregistrement de transaction pour chiffrer ledit enregistrement de signature de façon à prévoir un enregistrement chiffré pour fourniture au moyen de vérification de signature et de transaction.

2. Un appareil conformément à la revendication 1, caractérisé par un moyen pour réaliser un deuxième chiffrage dudit enregistrement numérique à l'aide d'une clé de chiffrage prédéterminée.

3. Un appareil conformément à la revendication 1 ou 2, caractérisé en ce que ledit premier moyen de génération comprend un style actionné manuellement (26), et un numériseur (46) pour capter et numériser les coordonnées dudit style (26).

4. Un appareil conformément à la revendication 3, caractérisé par un moyen d'affichage (48) pour présenter une image visuelle correspondant à ladite signature.

5. Un appareil conformément à la revendication 4, caractérisé en ce que le premier moyen de génération (20) comprend une surface de référence transparente (46) pour générer des signaux de captage de position en réponse au contact mobile par ledit style (26) qui est monté sur un afficheur à cristaux liquides (48) pour faire en sorte que ladite image visuelle soit présentée en repérage avec des points de contact successifs entre ladite surface (46) et ledit style (26).

6. Un appareil conformément à la revendication 5, caractérisé par un moyen de visualisation (50) pour afficher une image visuelle correspondant à ladite transaction.

7. Une méthode pour enregistrer une transaction, comprenant les étapes de

la génération d'un enregistrement de signature numérisé d'une signature approuvant la transaction, et de la génération d'un enregistrement de transaction numérisé représentatif de la transaction

caractérisée par l'étape de
la génération d'un enregistrement chiffré de la transaction pour fourniture à un moyen de vérification de la signature et de la transaction en utilisant ledit enregistrement de transaction numérisé pour chiffrer ledit enregistrement de signature.

8. Une méthode conformément à la revendication 7, caractérisée en ce que l'étape de la génération d'un enregistrement chiffré de la transaction comporte la sélection de données dudit enregistrement de transaction numérisé

et la réalisation d'une opération OU exclusif sur lesdites données par rapport audit enregistrement de signature numérisé.

FIG. 1

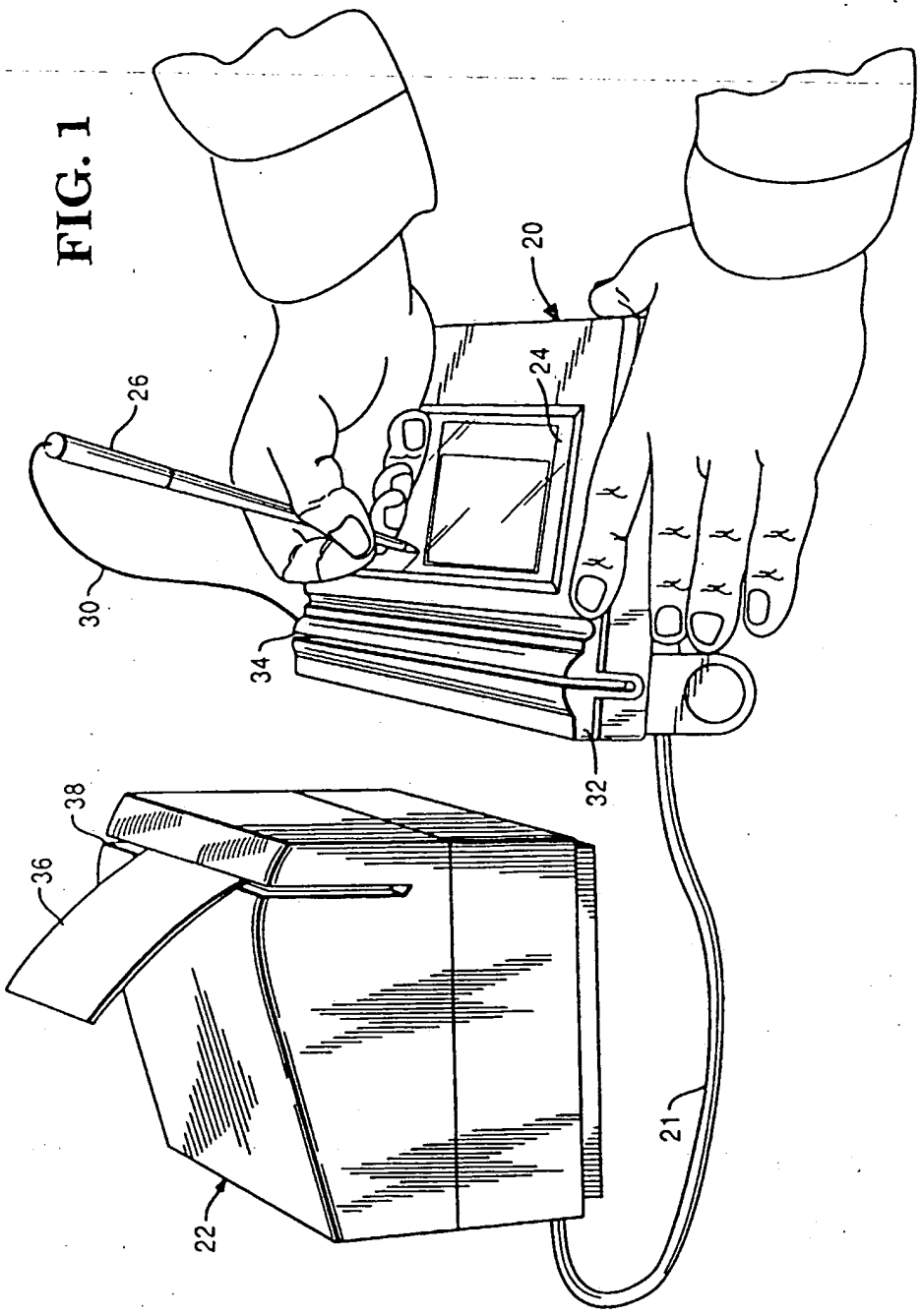


FIG. 2

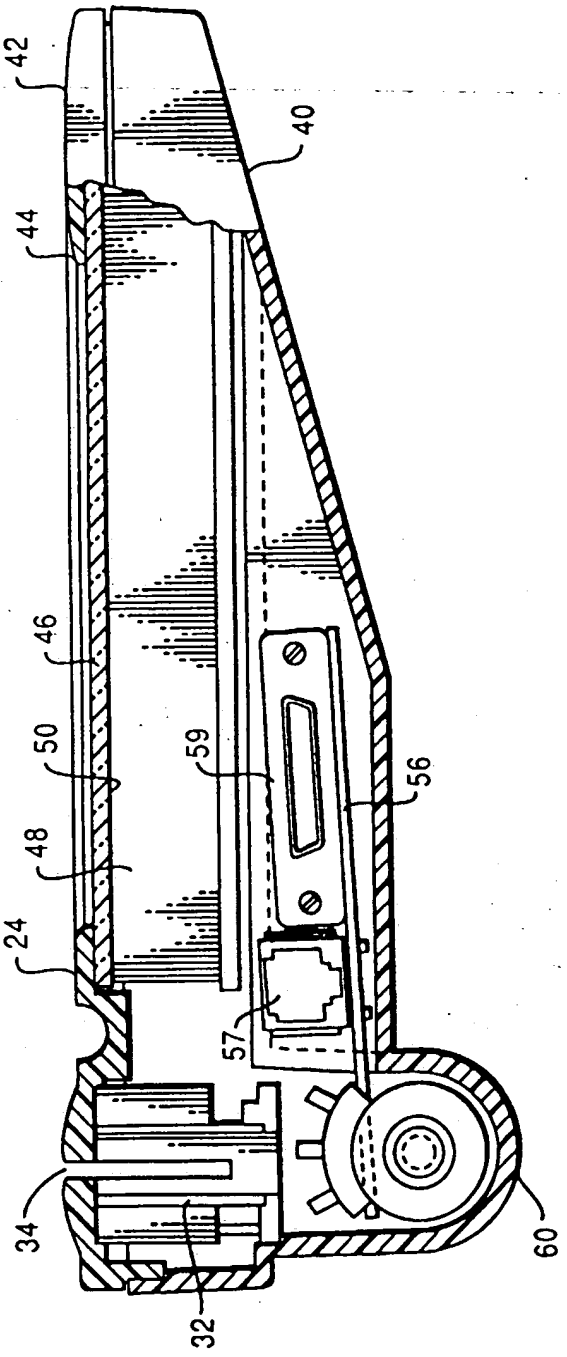


FIG. 3

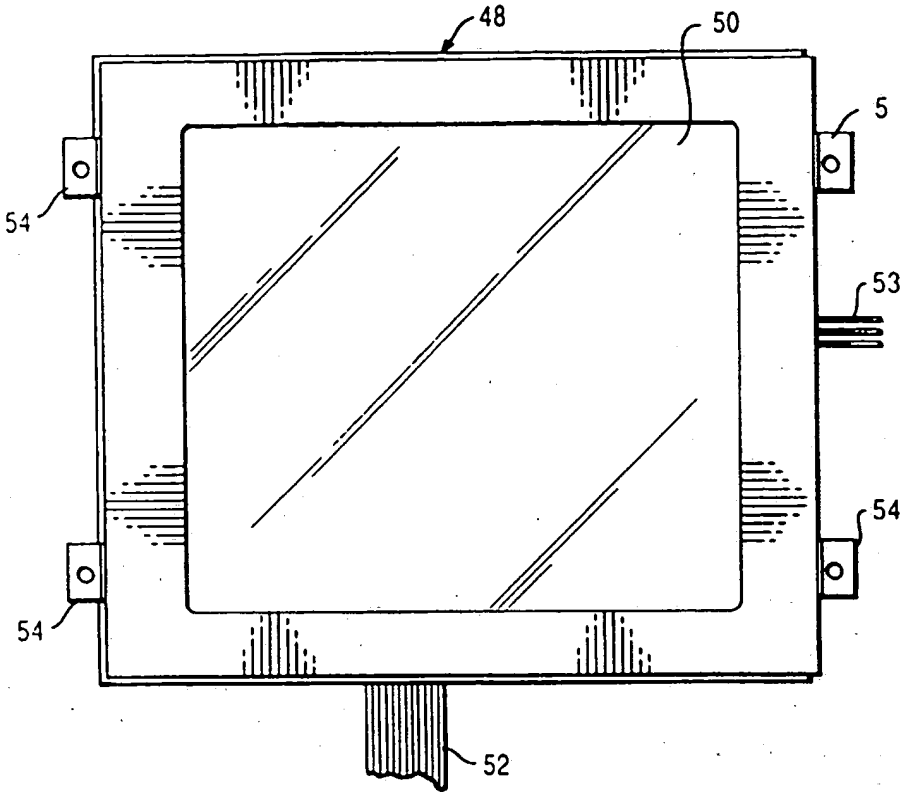


FIG. 4

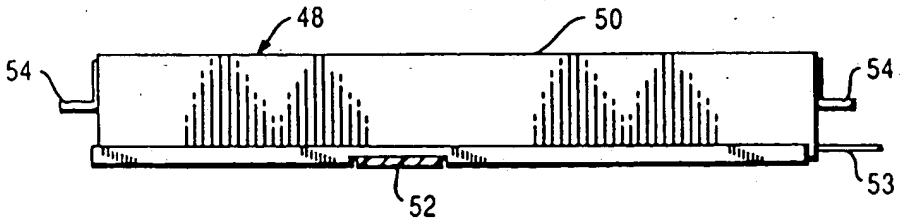


FIG. 5

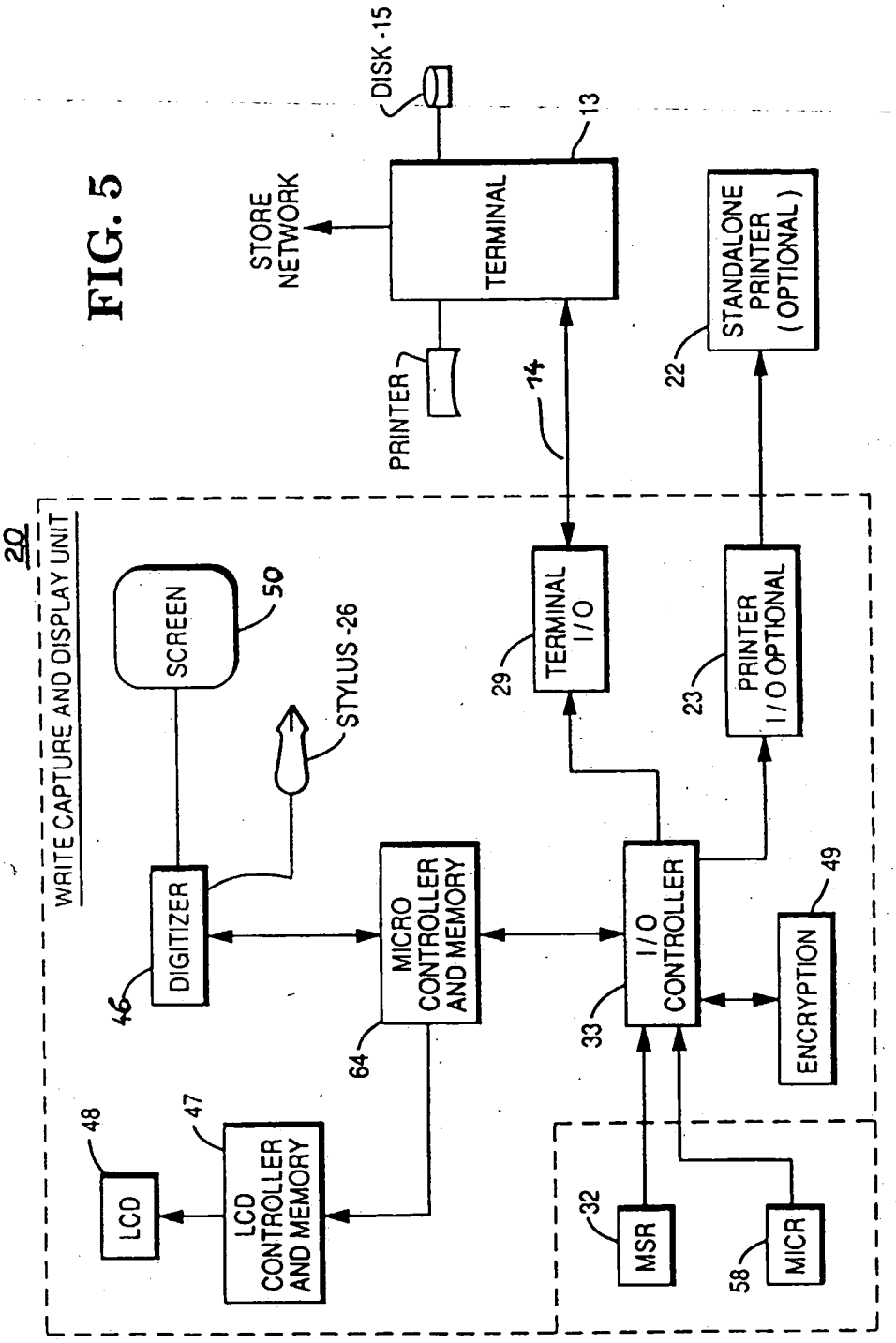

DISK -15
STORE NETWORK
TERMINAL
13
PRINTER
14
STANDALONE PRINTER (OPTIONAL)
22
20
WRITE CAPTURE AND DISPLAY UNIT
SCREEN
50
STYLUS -26
TERMINAL I/O
29
PRINTER I/O OPTIONAL
23
DIGITIZER
46
MICRO CONTROLLER AND MEMORY
64
I/O CONTROLLER
33
ENCRYPTION
49
LCD
48
LCD CONTROLLER AND MEMORY
47
MSR
32
MICR
58

FIG. 6

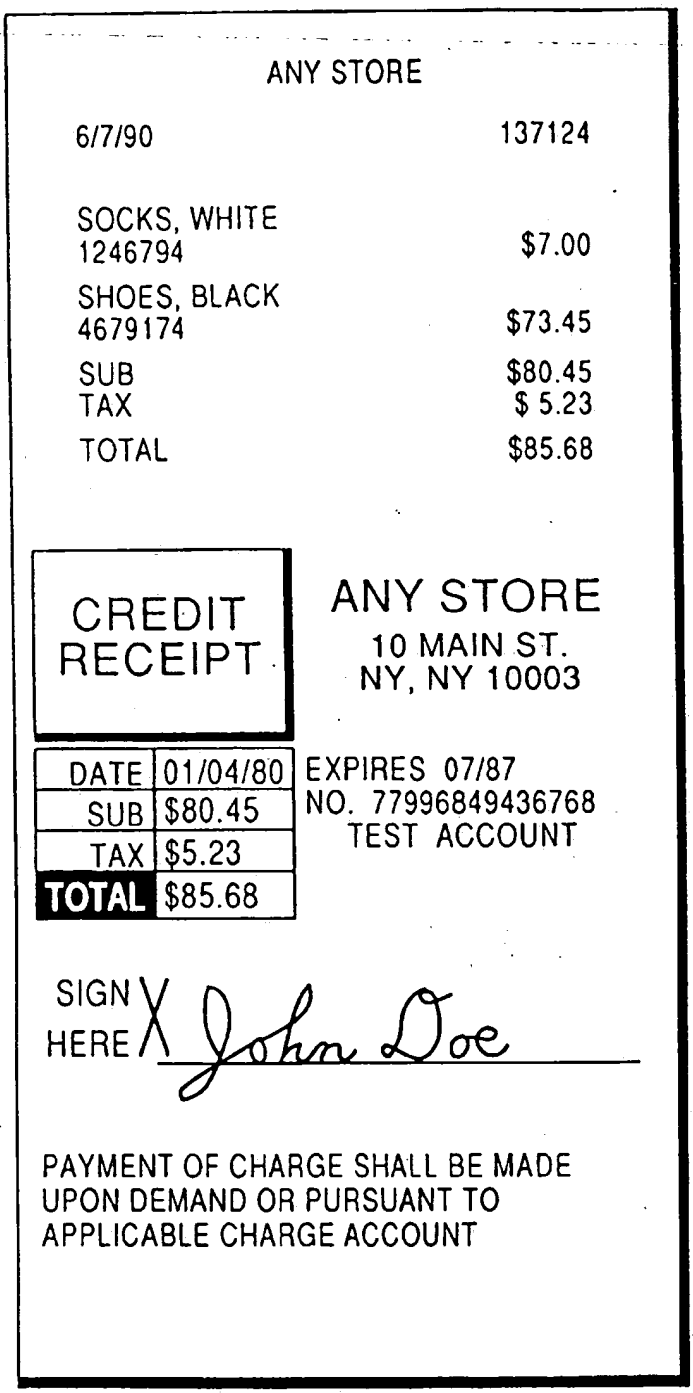

ANY STORE
6/7/90
137124
SOCKS, WHITE
1246794
$7.00
SHOES, BLACK
4679174
$73.45
SUB
$80.45
TAX
$ 5.23
TOTAL
$85.68
CREDIT RECEIPT
ANY STORE
10 MAIN ST.
NY, NY 10003
DATE 01/04/80
SUB $80.45
TAX $5.23
TOTAL $85.68
EXPIRES 07/87
NO. 77996849436768
TEST ACCOUNT
SIGN HERE X John Doe
PAYMENT OF CHARGE SHALL BE MADE UPON DEMAND OR PURSUANT TO APPLICABLE CHARGE ACCOUNT

FIG. 6A

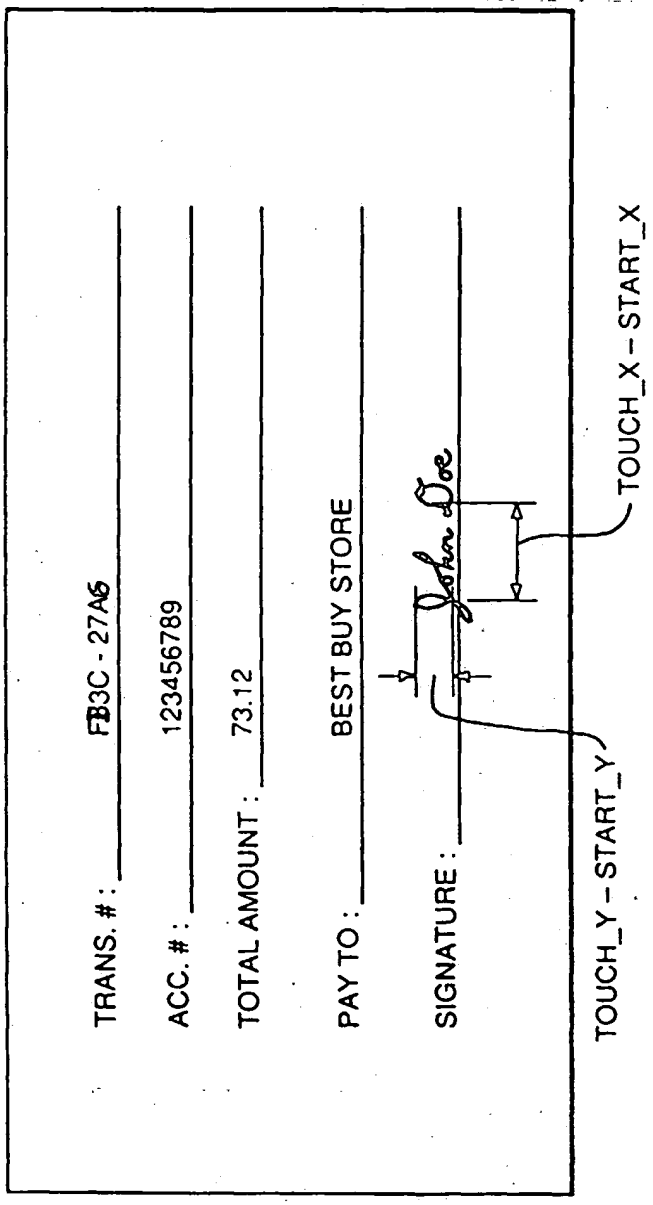
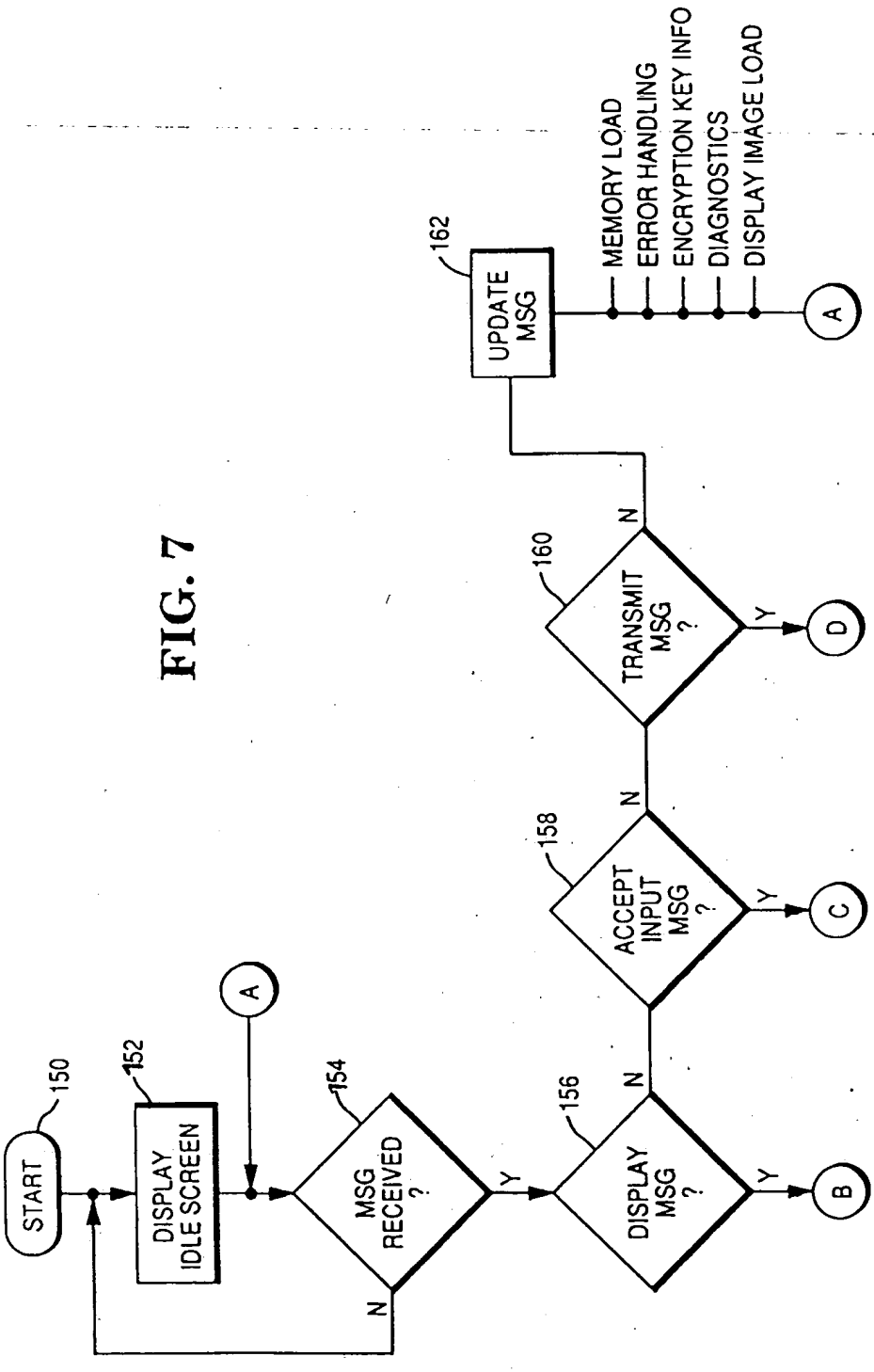

TRANS. # : FB3C - 27A6
ACC. # : 123456789
TOTAL AMOUNT : 73.12
PAY TO : BEST BUY STORE
SIGNATURE : John Doe
TOUCH_Y – START_Y
TOUCH_X – START_X

FIG. 7


START
150
DISPLAY IDLE SCREEN
152
A
MSG RECEIVED ?
154
N
Y
DISPLAY MSG ?
156
N
Y
B
ACCEPT INPUT MSG ?
158
N
Y
C
TRANSMIT MSG ?
160
N
Y
D
UPDATE MSG
162
MEMORY LOAD
ERROR HANDLING
ENCRYPTION KEY INFO
DIAGNOSTICS
DISPLAY IMAGE LOAD
A

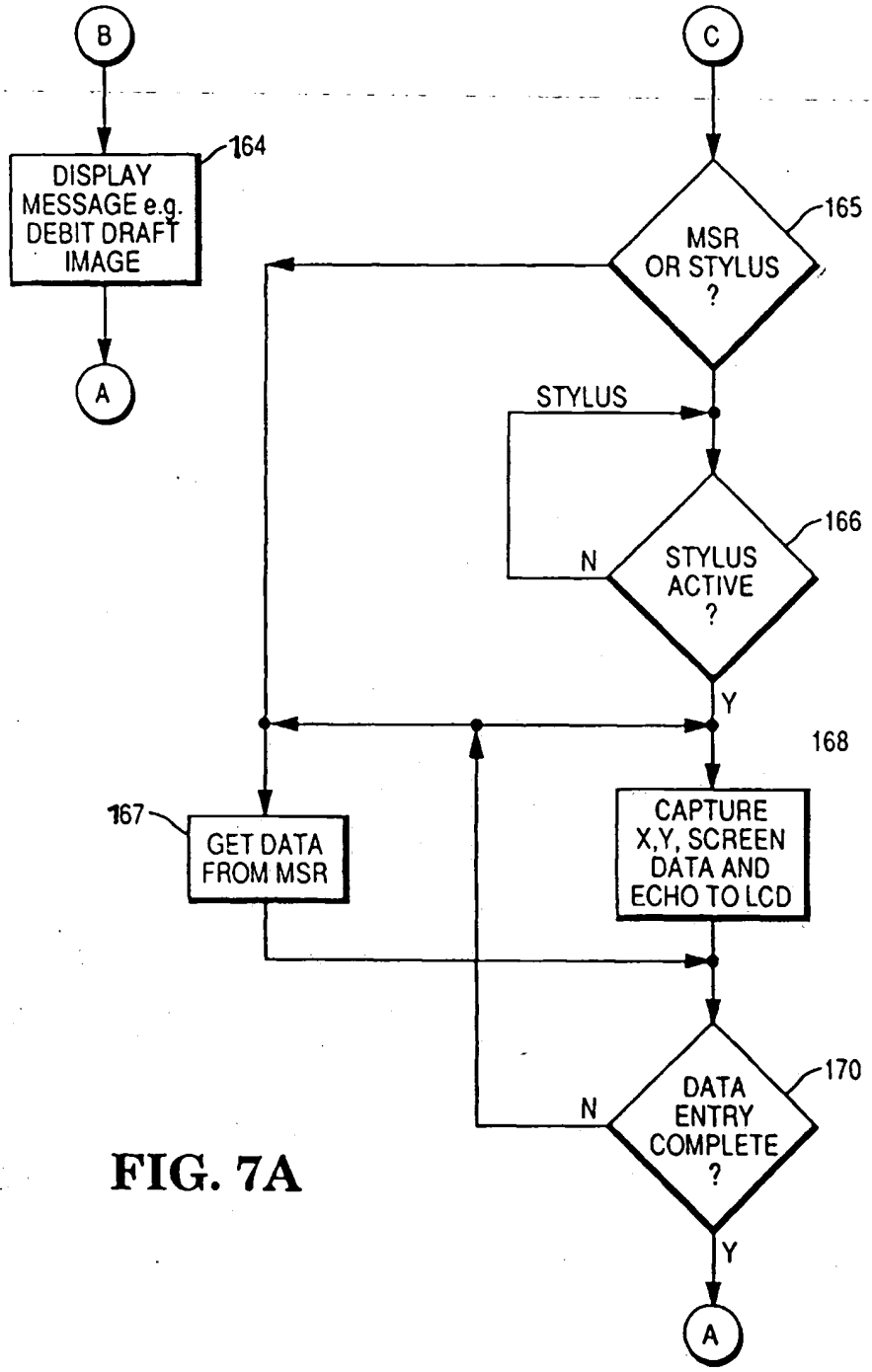

B
C
DISPLAY MESSAGE e.g. DEBIT DRAFT IMAGE
164
MSR OR STYLUS ?
165
A
STYLUS
STYLUS ACTIVE ?
166
N
Y
168
167
GET DATA FROM MSR
CAPTURE X,Y, SCREEN DATA AND ECHO TO LCD
DATA ENTRY COMPLETE ?
170
N
Y
A

FIG. 7A

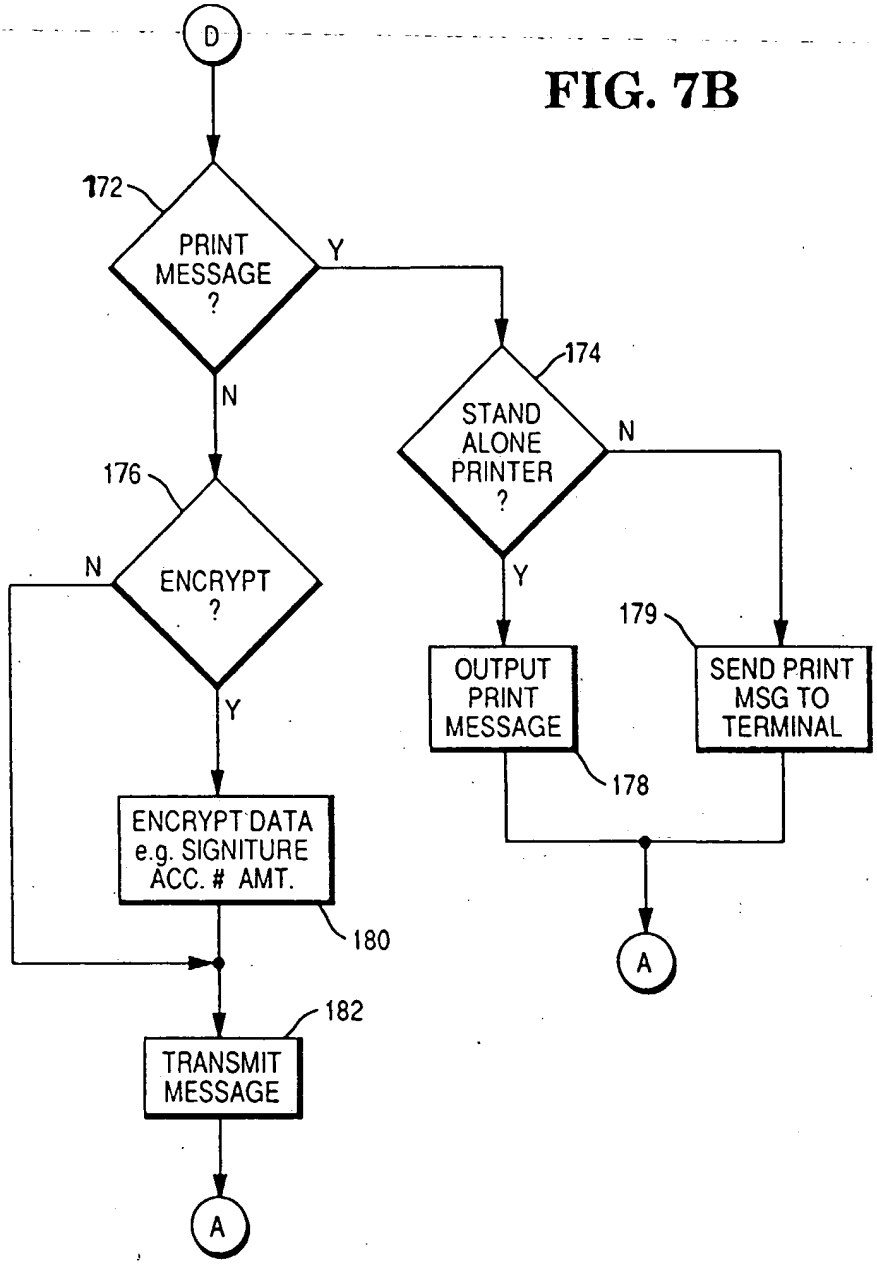

D
172
PRINT MESSAGE ?
Y
N
174
STAND ALONE PRINTER ?
N
Y
176
ENCRYPT ?
N
Y
179
OUTPUT PRINT MESSAGE
SEND PRINT MSG TO TERMINAL
178
ENCRYPT DATA e.g. SIGNITURE ACC. # AMT.
180
182
TRANSMIT MESSAGE
A
A

FIG. 7B

FIG. 8

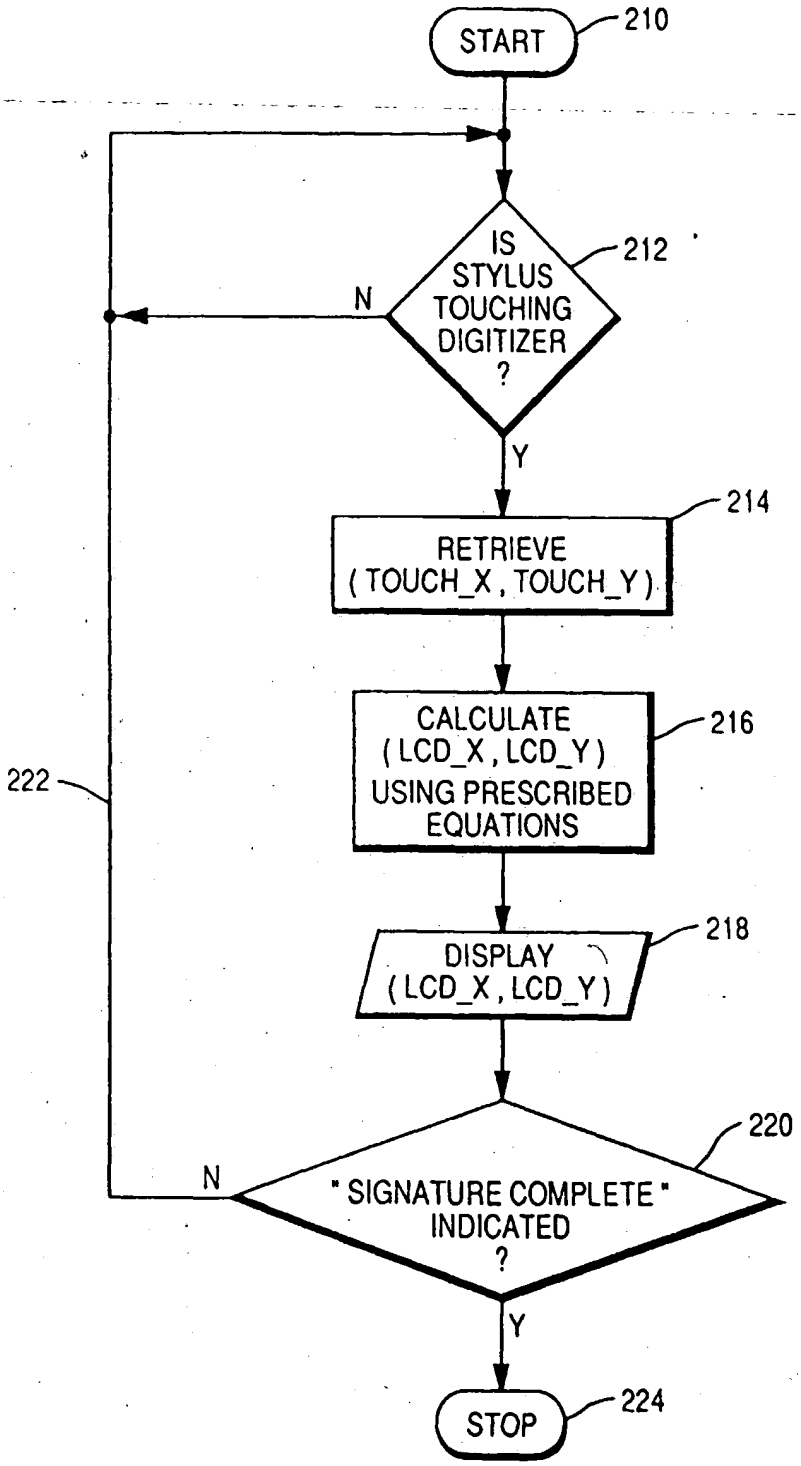
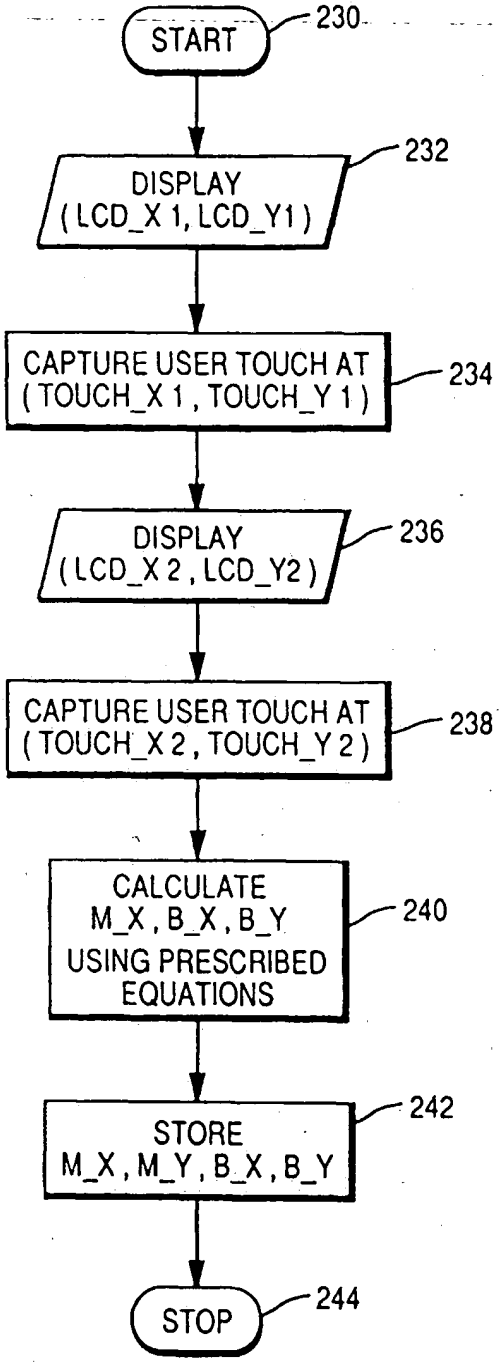

START
210
IS STYLUS TOUCHING DIGITIZER ?
212
N
Y
RETRIEVE (TOUCH_X , TOUCH_Y)
214
CALCULATE (LCD_X , LCD_Y) USING PRESCRIBED EQUATIONS
216
222
DISPLAY (LCD_X , LCD_Y)
218
" SIGNATURE COMPLETE " INDICATED ?
220
N
Y
STOP
224

FIG. 9


START
230
DISPLAY
(LCD_X 1, LCD_Y1)
232
CAPTURE USER TOUCH AT
(TOUCH_X 1 , TOUCH_Y 1)
234
DISPLAY
(LCD_X 2 , LCD_Y2)
236
CAPTURE USER TOUCH AT
(TOUCH_X 2 , TOUCH_Y 2)
238
CALCULATE
M_X , B_X , B_Y
USING PRESCRIBED
EQUATIONS
240
STORE
M_X , M_Y , B_X , B_Y
242
STOP
244